PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-XXXX
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Please type a plus sign (+) inside this box → [+]

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	CITI0131-US
First Inventor or Application Identifier	Cris T. PALTENGHE
Title	SYSTEM AND METHOD FOR SECURELY
Express Mail Label No.	

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] * Fee Transmittal Form *(e.g., PTO/SB/17)*
   (Submit an original and a duplicate for fee processing)

2. [X] Specification *[Total Pages* **24** *]*
   (preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure

3. [X] Drawing(s) *(35 U.S.C. 113)* *[Total Sheets* **6** *]*

4. Oath or Declaration *[Total Pages* **3** *]*
   a. [ ] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d))
      (for continuation/divisional with Box 16 completed)
      i. [ ] DELETION OF INVENTOR(S)
         Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. [ ] Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Copy
   b. [ ] Paper Copy (identical to computer copy)
   c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [ ] Assignment Papers (cover sheet & document(s))
8. [ ] 37 C.F.R.§3.73(b) Statement [ ] Power of *(when there is an assignee)* Attorney
9. [ ] English Translation Document *(if applicable)*
10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. [ ] * Small Entity Statement(s) [ ] Statement filed in prior application, Status still proper and desired *(PTO/SB/09-12)*
14. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. [ ] Other: ....
    ....

16. If a **CONTINUING APPLICATION**, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
    [ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: _____/_____
    Prior application information: Examiner _____ Group / Art Unit: _____
    For **CONTINUATION** or **DIVISIONAL APPS** only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label | *(Insert Customer No. or Attach bar code label here)* | or [X] Correspondence address below

Name	George T. Marcou
	Kilpatrick Stockton LLP
Address	700 Thirteenth Street, N.W.
	Suite 800

City	Washington	State	DC	Zip Code	20005
Country	US	Telephone	(202) 508-5800	Fax	(202) 508-5858

Name *(Print/Type)*	George T. Marcou	Registration No. *(Attorney/Agent)*	33,014
Signature	*(signature)* Reg. No. 41,668	Date	4/14/99

SYSTEM AND METHOD FOR SECURELY STORING
ELECTRONIC DATA

CROSS REFERENCE TO RELATED APPLICATIONS

5   This application is related to co-pending U.S. Provisional Patent Application
Serial No. 60/081,748, entitled "Virtual Wallet System", filed April 14, 1998; co-
pending U.S. Utility Patent Application Serial No. 09/190,993, entitled "Virtual
Wallet System", filed November 12, 1998; U.S. Utility Patent Application entitled
"System and Method for Controlling Transmission of Stored Information to Internet
10   Websites, Serial No. (not yet assigned) filed April 14, 1999; and, U.S. Utility Patent
Application entitled "Digital Graphic Signature System", Serial No. (not yet assigned)
filed April 13, 1999; all of which are incorporated herein by reference.

FIELD OF THE INVENTION

15   This invention relates generally to storage of electronic data, and more
particularly to a system and method for securely storing, managing and updating an
owner's data and accessing the stored data by a trusted party upon the occurrence of
an event, such as the death of the owner.

BACKGROUND

20   An electronic or virtual wallet is an embodiment of software acting as a
container for electronic objects, such as payment mechanisms, identity authentication
mechanisms, personal information and electronic artifacts of the owner. The
electronic or virtual wallet can reside, for example, on one or more of a consumer's
25   personal computer (PC), a server, and a smart card. The virtual wallet allows the
owner to control access to and distribution of information in the wallet, thereby
giving the owner security and total control over the owner's personal information.
Further, the virtual wallet provides mechanisms that eliminate the risk of loss of the
information in the wallet, for example, by remotely storing and/or disabling the wallet

contents. Thus, the virtual wallet is a trusted place to keep information and valuable financial items, as well as a convenient way to move information around.

Currently, many electronic wallets focus on payment mechanisms. However, electronic wallets can also be used to maintain, for example, identification information, authentication information, certificates, access keys, personal identification numbers (PIN's), and credit card, debit card and bank account information, as well as all other types of personal information of the owner, such as the owner's will. For a detailed discussion of a virtual or electronic wallet, see, for example, currently co-pending Provisional Patent Application Serial No. 60/081,748 filed on April 14, 1998 and Utility Patent Application Serial No. 09/190.993 filed on November 12, 1998, incorporated herein by reference. Information stored in an electronic wallet can be transmitted and received by the owner of the electronic wallet, for example, through the Internet or other types of networks.

Typically, a local aspect of the virtual wallet resides on the owner's personal computer (PC) and includes a certificate or other similar authentication instrument that allows the owner to remotely gain access to the entire virtual wallet which resides, for example, on a server. The local aspect of the virtual wallet updates the remote aspect of the virtual wallet with the latest information from the local aspect when the local wallet is on-line. The server also affords greater storage capacity for the owner's information than, for example, the owner's PC. Thus, the owner is able to define and have access to all the wallet functionality at sites where the local aspect of the wallet can be linked to the server, while the remote aspect of the wallet provides security for all of the information stored in the wallet.

However, the certificate or other similar authentication mechanism, such as a special PIN, password or key that allows the owner to gain access to the owner's electronic data securely stored in the virtual wallet may typically be known only to the owner. Therefore, upon the occurrence of an event, such as the death of the owner, which makes it impossible for the owner to act, if no other person knows how to access the stored information, it may be locked up forever.

SUMMARY OF THE INVENTION

It is a feature and advantage of the present invention to provide a system and method for securely updating and managing an owner's electronic data stored in the owner's virtual wallet.

It is another feature and advantage of the present invention to provide a system and method for updating technologies associated with the owner's data stored in the owner's virtual wallet when such technologies become outdated.

It is an additional feature and advantage of the present invention to provide a system and method for accessing the owner's data stored in the owner's virtual wallet upon the occurrence of an event, such as the death of the owner.

It is a further feature and advantage of the present invention to provide a system and method for making the contents of the owner's virtual wallet available to the owner's estate upon the death of the owner.

To achieve the stated and other features, advantages and objects of the present invention, an embodiment of the present invention provides a system and method for securely storing, managing and updating an owner's secret data and accessing the stored data by a trusted third party upon the occurrence of an event, such as the death of the owner. An embodiment of the present invention makes use of application software, such as a virtual wallet application running, for example, at least in part on the owner's personal computer and at least in part on a wallet server of a trusted third party, such as a bank or similar financial institution. The virtual wallet application also includes, for example, a virtual executor function and a virtual archivist function.

In an embodiment of the present invention, data is stored for the owner by the owner entering the data on the virtual wallet application at a terminal, such as the owner's personal computer, which is coupled to the wallet server over a network, or by receiving the data from another party, such as a merchant, lawyer, or the like, for the owner, by an electronic transmission, such as an electronic mail message. The network can be a private network or a public network, such as the internet. The types of secret information entered by the owner and stored for the owner by the virtual wallet application includes, for example, identification information, authentication

information, certificate information, access key information, PIN number information, credit card account information, debit card information, bank account information, and/or other personal information, such as will information, legal documents, insurance policies, brokerage account information, digital bearer instruments, digital

5 stock certificates, and digital bond certificates.

An embodiment of the present invention involves establishing the virtual wallet for the owner for various payment functions, as well as for storing the owner's secret data. The virtual wallet application automatically assigns the owner a secret device, such as a password, secret key, PIN number, or the like, for access by the

10 owner to the stored data, and automatically sends information about the secret device to the owner, for example, at the owner's terminal or PC coupled to the wallet server over the network. The owner's secret access device has, for example, two "flavors" or aspects, namely the owner's access aspect and the trusted third party's access aspect. The owner's access aspect is automatically sent to the owner, and the trusted third

15 party's access aspect is automatically stored by the virtual executor function of the virtual wallet application.

In an embodiment of the present invention, the third party's access aspect of the secret device is automatically escrowed by the virtual executor function of the virtual wallet application conditioned on the occurrence of an event affecting the

20 owner, which makes it impossible for the owner to act, such as the death or incompetence of the owner. Other secret access information is likewise automatically escrowed for the owner by the virtual executor function of the virtual wallet application, such as identification information, authentication information, certificate information, access key information, PIN number information, and password

25 information of the owner. Likewise, various decryption infrastructure is also automatically escrowed for the owner by the virtual executor function, such as public key cryptography infrastructure, electronic document infrastructure, digital signature infrastructure, user name infrastructure, password infrastructure, fingerprint scanner infrastructure, and secret key infrastructure of the owner.

In an embodiment of the present invention, upon the occurrence of the event, such as the death or incompetence of the owner, the owner's personal representative, such as the executor or trustee of the owner's estate, presents appropriate documentation to the trusted third party necessary to verify the occurrence of the event and the representative's authority to act. Verification of the occurrence of the event is entered on the virtual executor function of the owner's virtual wallet application, and the virtual executor function automatically provides access to the owner's stored data using the escrowed information, such as the trusted third party's access aspect of the owner's secret key.

An embodiment of the present invention also includes the virtual archivist function of the owner's virtual wallet, which automatically updates the technology aspects of the stored data from time to time. The technology aspects updated by the virtual archivist include, for example, technology relating to signing a document, encryption/decryption technology, technology related to a key for signing a document, technology related to reading a document itself, technology related to translation utilities used to make the documents themselves accessible, and technology related to a certificate revocation list. Other technology aspects updated by the virtual archivist include verification and validation technology to ensure that keys, digital certificates, and notary stamps are valid as of the time stamp date associated with the documents themselves.

Additional objects, advantages, and novel features of the invention will be set forth in part in the description that follows, and in part will become more apparent to those skilled in the art upon examination of the following, or may be learned by practicing the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows schematically an overview of key components, and the flow of information between the key components, for an embodiment of the present invention;

Fig. 2 is a table which illustrates examples of the types of data which the owner stores in the owner's virtual wallet for an embodiment of the present invention;

Fig. 3 is a table which shows examples of the types of information escrowed by the virtual executor for an embodiment of the present invention;

Fig. 4 is a table which shows examples of the two "flavors" for the key for accessing the owner's virtual wallet for an embodiment of the present invention;

Fig. 5 is a flow chart which amplifies the flow of information shown in Fig. 1 and provides further detail regarding the process of escrowing and accessing the owner's stored data for an embodiment of the present invention; and

Fig. 6 is a table which shows examples of the types of technologies which are updated by the virtual archivist for an embodiment of the present invention.

DETAILED DESCRIPTION

Referring now in detail to an embodiment of the present invention, an example of which is illustrated in the accompanying drawings, the present invention provides a system and method for securely storing, updating and managing an owner's electronic data and accessing the stored data by a trusted third party upon the occurrence of an event, such as the death or incompetence of the owner. Fig. 1 shows schematically an overview of key components, and the flow of information between the key components, for an embodiment of the present invention. The system for an embodiment of the present invention makes use of application software, such as a virtual wallet, which resides, for example, on one or both of the PC 2 of the owner 4 and a server 6 of a financial institution 8, such as a bank.

Fig. 2 is a table which illustrates examples of the types of data which the owner stores in the owner's virtual wallet for an embodiment of the present invention. Referring to Figs. 1 and 2, a local aspect 10 of the virtual wallet 12 residing on the owner's PC 2 allows the owner 4 to remotely gain access to the entire virtual wallet 14, which resides on the wallet server 6, over a network 16, such as the Internet. The local aspect 10 updates the remote aspect 14 of the virtual wallet 12 with the latest information from the local aspect when the local wallet is on-line to the server 6. Types of information which may be stored for the owner 4 in the virtual wallet 12 include, for example, identification information 18, authentication information 20,

certificates 22, access keys 24, personal identification numbers (PIN's) 26, credit card account information 28, debit card information 30, bank account information 32, and other personal information 34, such as the owner's will, legal documents, insurance policies, brokerage account information, digital bearer instruments, digital stock

5   certificates, and digital bond certificates.

Referring further to Fig. 1, a certificate or other similar authentication mechanism 36, such as a special PIN, password, or key, typically known only to the owner 4, allows the owner to gain access to the owner's electronic data securely stored in the virtual wallet 12. Generally, all of the digital services that are related to

10   electronic commerce, such as public key cryptography, electronic documents, and digital signatures, rely on the person who holds the certificate or who owns the wallet being present to access them. It can be as simple, for example, as a user name and password, if the owner 4 actually keeps the owner's password private. On the other hand, it can be as complicated as a fingerprint scanner requiring a live thumbprint that

15   has, for example, a body temperature. When the owner 4 dies, access to the owner's decryption infrastructure is likewise gone, and the access, in effect, dies with the owner.

A functionality within the virtual wallet for an embodiment of the present invention provides a solution to the problem by maintaining a file with all of this

20   critical information that can be opened by a trusted third party, such as the financial institution 8, e.g., a bank, upon the death of the owner 4. This allows for the settlement of all accounts and for access to information by the successors in interest of the owner 4. Referring again to Fig. 1, this aspect of an embodiment of the present invention, referred to as the virtual executor 38, allows access to the owner's secure

25   electronic data stored in the electronic wallet 12 once the owner 4 is, for example, deceased or legally incompetent or otherwise incapable of conducting her own affairs. Thus, the virtual executor 38 provides for the owner's secure information to be passed on to the owner's successors in interest after the owner 4 is, for example, deceased, incompetent, or otherwise unable to act on the owner's own behalf.

The virtual executor 38 functionality for an embodiment of the present invention provides a service that escrows the keys and/or similar access devices or mechanisms, so that when the owner 4 dies, the keys become part of the owner's estate and can be handled as part of the typical estate settlement. Fig. 3 is a table

5 which shows examples of the types of information escrowed by the virtual executor 38 for an embodiment of the present invention. The types of information escrowed by the virtual executor 38 include, for example, identification information 18, authentication information 20, certificates, 22, access keys 24, PIN numbers 26, passwords 40, and other similar secret access mechanisms 42. Without the virtual

10 executor 38, all of the owner's information that is protected, for example, by authentication information 20, keys 24, special PIN's 26, or passwords 40 may be forever locked up with the unavailability of the owner 4 to act, who is typically the only one who knows how to access the information stored in the virtual wallet 12.

In an embodiment of the present invention, the owner's secret keys and/or

15 other similar access devices are escrowed with the trusted third party which is, for example, the financial institution or bank 8, through the virtual executor 38, which is a type of virtual trust for the owner 4. The owner 4 escrows the owner's secret keys with the trusted third party 8, and the escrowed keys become part of the owner's estate. In other words, the escrowed keys are similar to the owner's will and all the

20 other trusts that the owner 4 may have. For example, the owner 4 can also have electronic funds, such as stored value or digital coins, that require the owner's thumbprint to decrypt. Upon the occurrence of an event, such as the death or incompetence of the owner, the system and method for an embodiment of the present invention provides a way for the trusted third party 8 to obtain access to the value that

25 is stored, for example, in those coins.

The system and method for an embodiment of the present invention provides, for example, a technology infrastructure associated with the virtual wallet 12 for accessing the contents of the virtual wallet, such as the owner's stored value in the wallet. The technology infrastructure associated with the virtual wallet 12 provides a

30 key that is durable and has, for example, two "flavors." Fig. 4 is a table which shows

examples of the two "flavors" for the key 44 for accessing the owner's virtual wallet 12 for an embodiment of the present invention. A first flavor of the key is the owner's secret access mechanism 36, which is necessary for the owner 4 to use every day for access to the virtual wallet 12. A second flavor 46 of the key is held by the trusted

5   third party 8 to give the third party access to the virtual wallet 12. The second flavor 46 is, in effect, like a master key that gives the trusted third party 8 access to the contents of the owner's virtual wallet 12 once the owner 4 is no longer able to use the owner's primary access device 36.

         Fig. 5 is a flow chart which amplifies the flow of information shown in Fig. 1

10   and provides further detail regarding the process of escrowing and accessing the owner's stored data for an embodiment of the present invention. At S1, the owner 4 at a terminal, such as the owner's PC 2, establishes the virtual wallet 12. At S2, the owner automatically receives a new key 36 that gives the owner access to the wallet. At S3, starting with that key 36, a key escrow is automatically created with the trusted

15   third party 8 by the virtual executor functionality 38 within the virtual wallet 12. The virtual executor functionality 38 automatically assures that the key 36 is appropriately escrowed. When an event occurs, such as the death of the owner 4, the owner's personal representative presents the appropriate notice about the owner's death, such as a death certificate, to the trusted third party 8 at S4, and the virtual executor 38 is

20   assured that the owner is actually deceased. At S5, the virtual executor 38 uses its set of keys to make available to the estate all of the content that the owner 4 has protected by those keys. For example, if it is the owner's access to digital funds within the owner's virtual wallet 12, one of those keys will allow access to those funds.

         In an embodiment of the present invention, in addition to secret keys, the

25   owner 4 may also have various other information stored in the virtual wallet 12, such as the owner's will 34. The owner 4 may have stored, for example, an electronic copy of the owner's will 34 in the data archive associated with the owner's virtual wallet 12 as the official copy of the will. Referring again to Fig. 5, at the death of the owner 4, the owner's personal representative takes a copy of the appropriate death certificate

30   and/or other appropriate documentation to prove the authority of the personal

representative and physically presents the documentation to the trusted third party 8. When the virtual executor 38 is assured of the owner's death, the virtual executor likewise uses its set of keys to make the owner's stored will 34 available to the owner's estate at S5. Demonstrating and documenting the owner's death, as well as the authority of the owner's personal representative to act upon the owner's death, to the trusted third party 8 is a part of the security mechanism for an embodiment of the present invention.

A further aspect for an embodiment of the present invention is a functionality within the virtual wallet 12, referred to as the virtual archivist, which provides for access and updating of the electronic information stored in the virtual wallet, for example, when various technologies associated with the stored information become outdated. Fig. 6 is a table which shows examples of the types of technologies which are updated by the virtual archivist for an embodiment of the present invention. The virtual archivist 46 updates technologies, such as those used to sign documents 48, encrypt/decrypt documents 50, keys 52, read the documents themselves 54, file translation utilities used to make the documents themselves accessible 55, and certificate revocation lists 56, to conform to changes in technology. The virtual archivist 46 also updates verification and validation technologies to ensure that keys 52, digital certificates 57, and notary stamps 60 are valid as of the time stamp date 58 associated with the documents themselves. Further, in an embodiment of the present invention, the virtual archivist 46 takes the information with the outdated technology and updates it to make it compatible with the latest technology, while maintaining the integrity of the original information. Thus, the virtual archivist 46 enables all information to conform to the latest technological advances.

For example, as electronic documents become, in effect, the original documents, the owner's will 34 stored electronically in the data archive part of the owner's virtual wallet 12 becomes the owner's official will. The owner's will written today may be written in an application, such as Word 7.0, which runs on an Intel Pentium computer with an operating system, such as Windows NT 4.0. If the owner 4 dies at a much later time in the future, it may be unlikely that a copy of Word 7.0, or

an Intel computer, or a copy of NT 4.0 will be readily available. Therefore, when the owner 4 dies in the future, in spite of the fact that the owner's will was signed and encrypted and protected and the owner has stored and archived all the keys so that the virtual executor has access to them, it may still not be possible to read the file because

5   the access mechanisms have ceased to exist.

In an embodiment of the present invention, the virtual archivist 46 is, in effect, a responsibility functionality. As the owner's files are archived in the data archive associated with the owner's virtual wallet 12, the virtual archivist 46 maintains the stored files in a way that the files can be accessed over time by automatically updating

10   the stored data and the technologies associated with the data as the technologies change over time. The virtual archivist 46 is part of one of the functionalities within the virtual wallet 12 that is the personal information archive. As the owner 4 inputs the owner's data into the data archive associated with the virtual wallet 12, the virtual archivist 46 is automatically informed of what the owner's data is and automatically

15   formats the data, so the data can continue to be useful.

Various preferred embodiments of the invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the

20   art without departing from the spirit and scope of the present invention. Accordingly, the invention is limited only by the following claims.

12

What is claimed is:

1.   A method for securely storing data for an owner, comprising:

storing the data for the owner;

automatically assigning a secret device to the owner for accessing the stored data;

automatically escrowing the secret device conditioned on the occurrence of an event;

receiving verification of the occurrence of the event; and

accessing the stored data with the escrowed secret device.

2.   The method of claim 1, wherein storing the data further comprises entering the data on a virtual wallet application for the owner.

3.   The method of claim 2, wherein entering the data further comprises entering the data by the owner at a terminal.

4.   The method of claim 3, wherein entering the data further comprises entering the data by the owner at the terminal coupled to a server.

5.   The method of claim 4, wherein the terminal further comprises a personal computer.

6.   The method of claim 4, wherein the server further comprises the server of a trusted third party.

7.   The method of claim 6, wherein the trusted third party's server further comprises a financial institution server.

1   8.   The method of claim 7, wherein the financial institution further
2   comprises a bank.

1   9.   The method of claim 4, wherein entering the data further comprises
2   entering the data by the owner at the terminal coupled to the server over a network.

1   10.   The method of claim 9, wherein the network further comprises a
2   private network.

1   11.   The method of claim 9, wherein the network further comprises a public
2   network.

1   12.   The method of claim 11, wherein the public network further comprises
2   the internet.

1   13.   The method of claim 2, wherein entering the data further comprises
2   entering the data for the owner on the virtual wallet application having a virtual
3   executor function.

1   14.   The method of claim 2, wherein entering the data further comprises
2   entering the data for the owner on the virtual wallet application having a virtual
3   archivist function.

1   15.   The method of claim 1, wherein storing the data further comprises
2   entering the data by the owner at a terminal.

1   16.   The method of claim 15, wherein the terminal further comprises a
2   personal computer.

17. The method of claim 15, wherein entering the data further comprises entering the data by the owner at the terminal coupled to a server.

18. The method of claim 17, wherein entering the data further comprises entering the data on a virtual wallet application residing at least in part on the server.

19. The method of claim 17, wherein entering the data further comprises entering the data on a virtual wallet application residing at least in part on the terminal.

20. The method of claim 1, wherein storing the data further comprises storing at least one category of information by a virtual wallet application for the owner selected from a group of information consisting of identification information, authentication information, certificate information, access key information, PIN number information, credit card account information, debit card information, bank account information, and other personal information.

21. The method of claim 1, wherein assigning the secret device further comprises automatically assigning the secret device to the owner by a virtual wallet application.

22. The method of claim 21, wherein automatically assigning the secret device further comprises automatically assigning the secret device to the owner at a terminal.

23. The method of claim 22, automatically assigning the secret device further comprises automatically assigning the secret device by the virtual wallet application residing at least in part on a server coupled to the terminal.

1   24. The method of claim 23, wherein the terminal further comprises a
2 personal computer.

1   25. The method of claim 23, wherein the server further comprises the
2 server of a trusted third party.

1   26. The method of claim 25, wherein the trusted third party's server further
2 comprises a financial institution server.

1   27. The method of claim 26, wherein the financial institution further
2 comprises a bank.

1   28. The method of claim 23, wherein automatically assigning the secret
2 device further comprises automatically sending information about the secret device to
3 the owner at the terminal coupled to the server over a network.

1   29. The method of claim 28, wherein the network further comprises a
2 private network.

1   30. The method of claim 28, wherein the network further comprises a
2 public network.

1   31. The method of claim 30, wherein the public network further comprises
2 the internet.

1   32. The method of claim 1, wherein automatically assigning the secret
2 device further comprises automatically assigning the secret device with at least two
3 access aspects.

33. The method of claim 32, wherein automatically assigning the secret device further comprises automatically assigning the secret device with an owner's access aspect and a trusted third party's access aspect.

34. The method of claim 33, wherein automatically assigning the owner's access aspect further comprises automatically sending the owner's access aspect to the owner.

35. The method of claim 33, wherein automatically assigning the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect.

36. The method of claim 35, wherein automatically storing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by a virtual wallet application for the owner.

37. The method of claim 36, wherein automatically storing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by a virtual executor function of the virtual wallet application for the owner.

38. The method of claim 37, wherein automatically storing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by the virtual executor function of the virtual wallet application on a server of the trusted third party.

39. The method of claim 38, wherein the trusted third party server further comprises a financial institution computer.

1   40.   The method of claim 39, wherein the financial institution further
2   comprises a bank.

1   41.   The method of claim 1, wherein automatically escrowing the secret
2   device further comprises automatically escrowing a trusted third-party's access aspect
3   of the secret device for the owner.

1   42.   The method of claim 41, wherein automatically escrowing the trusted
2   third party's access aspect further comprises automatically storing the trusted third
3   party's access aspect by a virtual wallet application for the owner.

1   43.   The method of claim 42, wherein automatically storing the trusted third
2   party's access aspect further comprises automatically storing the trusted third party's
3   access aspect by a virtual executor function of the virtual wallet.

1   44.   The method of claim 41, wherein automatically escrowing the trusted
2   third party's access aspect further comprises automatically storing the trusted third
3   party's access aspect conditioned on the occurrence of the event affecting the owner.

1   45.   The method of claim 44, wherein the event affecting the owner further
2   comprises the owner's death.

1   46.   The method of claim 44, wherein the event affecting the owner further
2   comprises the owner's incompetence.

1   47.   The method of claim 1, wherein automatically escrowing the secret
2   device further comprises automatically escrowing secret access information for the
3   owner.

48. The method of claim 47, wherein automatically escrowing secret access information further comprises automatically storing at least one type of secret access information selected from a group of secret access information consisting of identification information, authentication information, certificate information, access key information, PIN number information, and password information.

49. The method of claim 1, wherein automatically escrowing the secret device further comprises automatically escrowing decryption infrastructure for the owner.

50. The method of claim 49, wherein automatically escrowing decryption infrastructure further comprises automatically storing at least one decryption infrastructure selected from a group of decryption infrastructure consisting of public key cryptography infrastructure, electronic document infrastructure, digital signature infrastructure, user name infrastructure, password infrastructure, fingerprint scanner infrastructure, and secret key infrastructure.

51. The method of claim 1, wherein receiving the verification further comprises receiving the verification by a trusted third party for the owner.

52. The method of claim 1, wherein receiving the verification further comprises receiving the verification from a personal representative of the owner.

53. The method of claim 1, wherein receiving the verification further comprises receiving the verification of an event affecting the owner.

54. The method of claim 53, wherein the event affecting the owner further comprises the owner's death.

1   55.   The method of claim 53, wherein the event affecting the owner further

2   comprises the owner's incompetence.

1   56.   The method of claim 1, wherein receiving the verification further

2   comprises entering the verification of the occurrence of the event on a virtual wallet

3   application of the owner.

1   57.   The method of claim 56, wherein entering the verification further

2   comprises entering the verification on a virtual executor function of the virtual wallet

3   application.

1   58.   The method of claim 57, wherein entering the verification further

2   comprises entering the verification on the virtual executor function of the virtual

3   wallet application on a server.

1   59.   The method of claim 58, wherein entering the verification further

2   comprises entering the verification on the virtual executor function of the virtual

3   wallet application on the server of a trusted third party.

1   60.   The method of claim 59, wherein the trusted third party further

2   comprises a financial institution.

1   61.   The method of claim 60, wherein the financial institution further

2   comprises a bank.

1   62.   The method of claim 1, wherein accessing the stored data further

2   comprises accessing the data stored in a virtual wallet application of the owner.

1   63.   The method of claim 62, wherein accessing the stored data further

2   comprises accessing the data stored in a virtual executor function of the virtual wallet

3   application on a server.

1   64.   The method of claim 63, wherein accessing the stored data further

2   comprises accessing the data stored in the virtual executor function of the virtual

3   wallet application on the server of a trusted third party.

1   65.   The method of claim 64, wherein the trusted third party further

2   comprises a financial institution.

1   66.   The method of claim 65, wherein the financial institution further

2   comprises a bank.

1   67.   The method of claim 1, wherein accessing the stored data further

2   comprises accessing the data using a trusted third party's access aspect of the secret

3   device.

1   68.   The method of claim 67, wherein accessing the data further comprises

2   accessing the data using the trusted third party's access aspect of the secret device

3   stored by a virtual executor function of a virtual wallet application.

1   69.   The method of claim 68, wherein accessing the data further comprises

2   accessing the data using the trusted third party's access aspect of the secret device

3   stored by the virtual executor function of the virtual wallet application on a server of

4   the trusted third party.

1   70.   The method of claim 69, wherein the trusted third party further

2   comprises a financial institution.

1   71.   The method of claim 70, wherein the financial institution further

2   comprises a bank.

1   72.   The method of claim 1, further comprising automatically updating

2   technology aspects of the stored data.

1   73.   The method of claim 72, wherein automatically updating the

2   technology aspects further comprises automatically updating technology aspects of the

3   data by a virtual archivist function of a virtual wallet application.

1   74.   The method of claim 73, wherein automatically updating the

2   technology aspects by the virtual archivist function further comprises automatically

3   updating the technology aspects by the virtual archivist function of the virtual wallet

4   application on a server.

1   75.   The method of claim 74, wherein automatically updating the

2   technology aspects further comprises automatically updating the technology aspects

3   by the virtual archivist function of the virtual wallet application on the server of a

4   trusted third party.

1   76.   The method of claim 75, wherein the trusted third party further

2   comprises a financial institution.

1   77.   The method of claim 76, wherein the financial institution further

2   comprises a bank.

1   78.   The method of claim 1, wherein automatically updating the technology

2   aspects further comprises automatically updating at least one technology aspect of the

3   data selected from a group of technology aspects consisting of technology related to

4   signing a document, encryption technology, technology related to a key for signing a

5 document, technology related to a document itself, technology related to a certificate

6 revocation list, technology related to a time stamp, and technology related to a notary

7 stamp.

1   79.   The method of claim 1, wherein storing the data further comprises

2 receiving the data from another party by a virtual wallet application for the owner.

1   80.   The method of claim 79, wherein receiving the data further comprises

2 receiving the data by the virtual wallet application for the owner by electronic mail.

1   81.   A system for securely storing data for an owner, comprising:

2   means for storing the data for the owner;

3   means associated with the storing means for automatically assigning a

4 secret device to the owner for accessing the stored data;

5   means associated with the storing means for automatically escrowing

6 the secret device conditioned upon the occurrence of an event;

7   means associated with the storing means for receiving verification of

8 the occurrence of the event; and

9   means associated with the storing means for accessing the stored data

10 with the escrowed secret device.

1   82.   The system of claim 81, wherein the means for storing the data further

2 comprises a server.

1   83.   The system of claim 82, wherein the server further comprises the server

2 of a trusted third party.

1   84.   The system of claim 83, wherein the means for storing the data further

2 comprises a terminal coupled to the server.

1   85.   The system of claim 84, wherein the means for storing the data further

2   comprises a network coupling the terminal to the server.

1   86.   The system of claim 81, wherein the means for automatically assigning

2   the secret device further comprises a server.

1   87.   The system of claim 86, wherein the server further comprises the server

2   of a trusted third party.

1   88.   The system of claim 81, wherein the means for automatically assigning

2   the secret device further comprises the server coupled to a terminal over a network.

1   89.   The system of claim 81, wherein the means for receiving the

2   verification further comprises a server.

1   90.   The system of claim 89, wherein the server further comprises the server

2   of a trusted third party.

1   91.   The system of claim 81, wherein the means for accessing the stored

2   data further comprises a server.

1   92.   The system of claim 91, wherein the server further comprises the server

2   of a trusted third party.

ABSTRACT

A system and method for securely storing data provides for storing, managing, and updating an owner's secret data and for accessing the stored data by a trusted third party upon the occurrence of an event, such as the death of the owner. The system and method makes use of application software, such as a virtual wallet running at least in part on the server of a trusted third party and with a virtual executor function and a virtual archivist function. The virtual executor function automatically escrows a trusted third party's access aspect of the owner's secret device for accessing the stored data. Upon verification of the occurrence of the event, the virtual executor provides access to the stored data using the trusted third party's access aspect. The virtual archivist function automatically updates technologies related to the stored data.

Trusted Third Party

8

Virtual Wallet
Server

Remote Aspect of
Virtual Wallet — 14

Virtual
Executor — 38

Virtual
Archivist — 46

6

NETWORK

16

PC

2

Local Aspect of Virtual
Wallet — 10

Owner

4

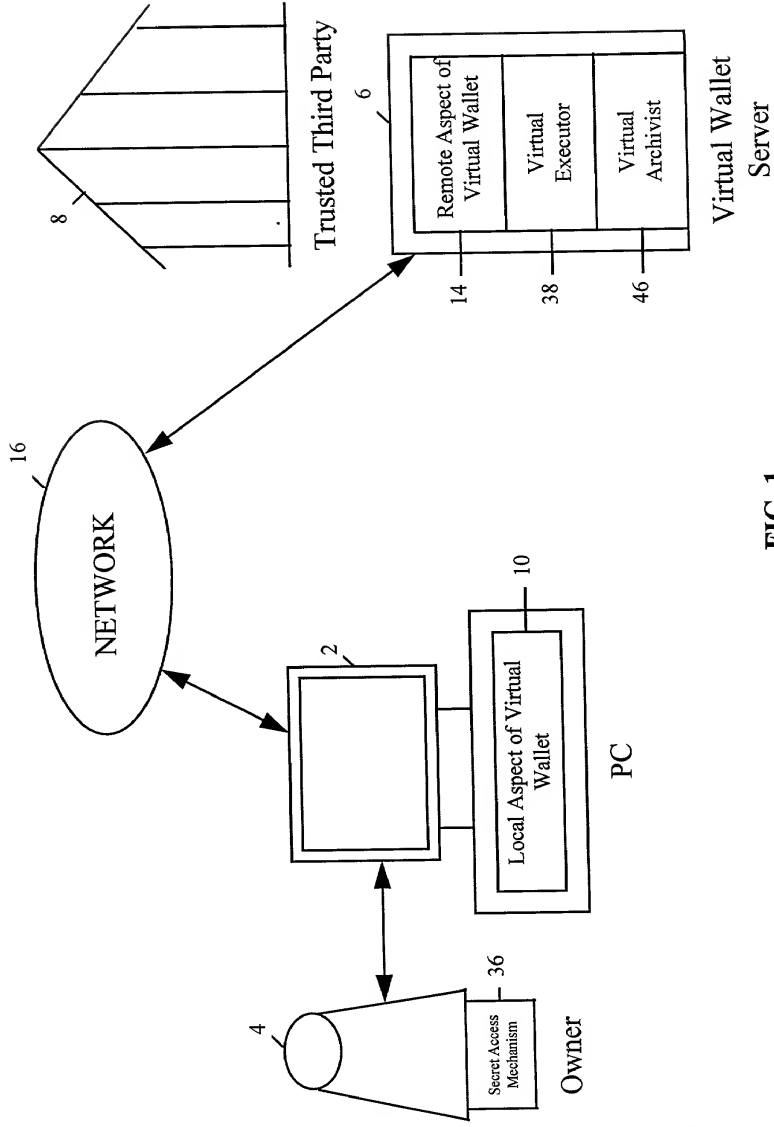Secret Access
Mechanism — 36

FIG. 1

VIRTUAL WALLET — 12

Identification Information — 18

Authentication Information — 20

Certificates — 22

Access Keys — 24

PIN Numbers — 26

Credit Card Account Information — 28

Debit Card Account Information — 30

Bank Account Information — 32

Other Personal Information — 34

FIG. 2

VIRTUAL EXECUTOR— 38

Identification Information — 18

Authentication Information — 20

Certificates — 22

Access Keys — 24

PIN Numbers — 26

Passwords — 40

Other Secret Access Mechanisms — 42

FIG. 3

KEY "FLAVORS" FOR ACCESSING VIRTUAL WALLET

44

Owner's Access	36
Trusted Third-Party's Access	46

FIG. 4

| S1 | Owner Establishes Virtual Wallet |

| S2 | Owner Receives Secret Key |

| S3 | Virtual Executor Escrows Secret Key |

| S4 | Virtual Executor Receives Notice of Event, Such as Owner's Death |

| S5 | Virtual Executor Makes Contents Protected by Keys Available to Owner's Estate Using Escrowed Keys |
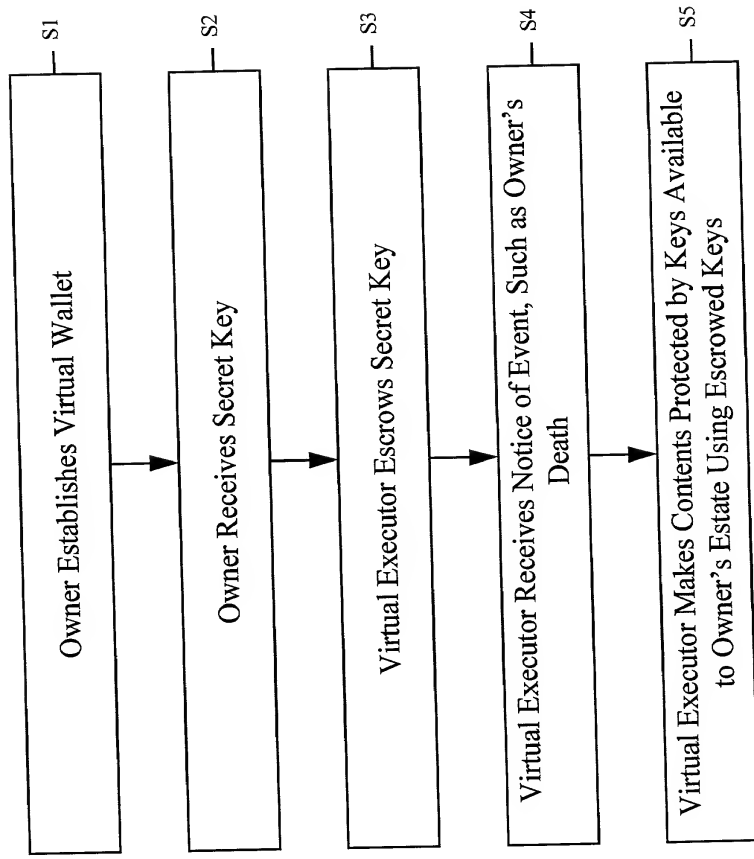
FIG. 5

VIRTUAL ARCHIVIST— 46

Technologies Used to Sign Documents	48
Technology to Encrypt/Decrypt	50
Keys for Signing Documents	52
Documents Themselves	54
File Translation Utilities	55
Certificate Revocation Lists	56
Digital Certificates	57
Time Stamps	58
Notary Stamps	60

FIG. 6

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled <u>SYSTEM AND METHOD FOR SECURELY STORING ELECTRONIC DATA</u>; the specification of which (check one)

___X___ is attached hereto.

_____ was filed on_____ as

___ Application Serial No. _____

_____ and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent of inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)   Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which be came available between the filing date of the prior application and the national or PCT international filing date of this application:

60/081,748	April 14, 1998	Pending
(Application Serial No.)	(Filing Date)	(Status - patented, pending, abandoned)
09/190,993	November 12, 1998	Pending
(Application Serial No.)	(Filing Date)	(Status - patented, pending, abandoned)
	April 13, 1999	Pending
(Application Serial No.)	(Filing Date)	(Status - patented, pending, abandoned)
	April 14, 1999	Pending
(Application Serial No.)	(Filing Date)	(Status - patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

English Language Declaration

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

George T. Marcou, Registration No. 33,014; Richard Peterson, Registration No. 35,320; Wilburn L. Chesser, Registration No. 41,668; Benjamin Driscoll, Registration No. 41,571, Charles W. Calkins, Registration No. 31,814, John M. Harrington, Registration No. 25,592, Whitney R. Winston, Registration No. P-44,432, Dawn-Marie Bey, Registration No. P-44,442, and John Ball, Registration No. P-44,433.

Send Correspondence to: Direct telephone calls to:

George T. Marcou   George T. Marcou
Kilpatrick Stockton LLP   (202) 508-5800
Suite 800
700 - 13th Street, N.W.
Washington, D.C. 20005

Full name of first inventor: Cris T. PALTENGHE	
First Inventor's Signature	Date
Residence: 11718 Entrada Avenue, Northridge, CA 91326	
Citizenship: USA	
Post Office Address: 11718 Entrada Avenue, Northridge, CA 91326	
Full name of second inventor: Alnoor B. MAMDANI	
Second Inventor's Signature	Date
Residence: 2030 Penmar Avenue, Venice, CA 90291	
Citizenship: USA	
Post Office Address: 2030 Penmar Avenue, Venice, CA 90291	

Full name of third inventor: Lisa EZROL
Third Inventor's Signature   Date
Residence: 525 East 72nd Street, Apt. 42A, New York, NY 10021
Citizenship: USA
Post Office Address: 525 East 72nd Street, Apt. 42A, New York, NY 10021

Full name of fourth inventor: Charles GOLVIN
Fourth Inventor's Signature   Date
Residence: 2762 McConnell Drive, Los Angeles, CA 90064
Citizenship: USA
Post Office Address: 2762 McConnell Drive, Los Angeles, CA 90064

Full name of fifth inventor: Henry LICHSTEIN
Fifth Inventor's Signature   Date
Residence: 544 Dryad Road, Santa Monica, CA 90402
Citizenship: USA
Post Office Address: 544 Dryad Road, Santa Monica CA 90402

Full name of sixth inventor: Melvin Michio TAKATA
Sixth Inventor's Signature   Date
Residence: 855 Paseo Del Robledo, Thousand Oaks, CA 91360
Citizenship: USA
Post Office Address: 855 Paseo Del Robledo, Thousand Oaks, CA 91360